DATA MANAGEMENT PLAN GUIDELINES

The data management plan guidelines contain four steps. You are being asked to describe the actions that you will take to address these protections specific to this research request.

The exhibit below is an illustration of the four steps of the data management plan and the corresponding data privacy safeguards.

DATA MANAGEMENT PROCESS	DATA PRIVACY AND SECURITY SAFEGUARDS		
	Organizational Safeguards	Personnel/Staffing Safeguards	Technical Safeguards
Possession and Storage of CMS data files	✓	✓	✓
Data Sharing/Electronic Transmission	✓	✓	✓
Data Reporting/Publication	✓		
Completion of Research Tasks and Data Destruction	✓	✓	✓

The safeguards you describe should be reasonable and appropriate based on the organizational environment in which your research is conducted.

Please note that your explanation should fully describe the protections you have in place. We expect that some of your safeguard descriptions in response to a step may overlap with another step. CMS is not requesting documentation that supports your descriptions at this time. Researchers should maintain documentation supporting this data management plan should CMS request a remote review or on-site visit.

The safeguards you describe in this plan are specific to this research request. You will find several examples of safeguards following each step that may or may not apply to your particular research data management environment for this request. These are simply examples to assist you. Following the guidance, you will find an appendix (pages 4-5) that provide scenarios and references that may provide further assistance. Some organizations may have documents on file such as a Self Assessment or Information System Security Plan. Please feel free to refer to these documents to develop your data management plan.

STEP 1: PHYSICAL POSSESSION AND STORAGE OF CMS DATA FILES

GOAL

In this step, you should describe the data privacy protections you have in place for conducting this research. Your description should include discussion about how you will maintain an inventory of CMS data files and manage physical access to them for the duration of your DUA.

Explain your organizational safeguards. Examples are:

- How you manage/maintain an inventory of the data files and keep it up to date
- Data sharing agreements among organizations (both internal and external to your organization) to ensure protections are being applied throughout the DUA lifecycle

Explain your personnel/staffing safeguards. Examples are:

- Confidentiality agreements that you have in place with individuals you have identified as being assigned to this study. Include, for example, agreements between the Principal Investigator

(PI)/Data Custodian and others, including research team members, computer/information Technology (IT) support staff, secretarial/administrative staff and volunteers. (*Note: all volunteers assisting with the project must have a direct reporting relationship with a lead researcher)*

- How you will keep CMS informed of project staffing changes as related to data custodianship
- Staff training programs you have in place to ensure data protections and stewardship responsibilities are communicated to the research team
- Procedures you use to track the active status and roles of each member of the research team throughout the DUA period

Explain your technical and physical safeguards. Examples are:

- Actions you have taken to physically secure storage of data files, such as site and office access controls, secured file cabinets and locked offices
- Safeguards you have put in place to limit access to personally identifiable information (PII)among the research team, , such as analytical data extracts (*Note: if the distribution of analytical data extracts among your researchers is part of your data management plan, the extracts remain s subject to the terms of Section #9 of your DUA)*
- Provide a brief summary about the network where CMS data will reside
- Written policies and procedures for ensuring that data are protected when contained on:
  - servers and local workstations
  - hard media devices (CDS, DVDs, hard drives, etc.) or your organization's standards for the physical removal, transfer or disclosure of data

STEP 2: DATA SHARING, ELECTRONIC TRANSMISSION, AND DISTRIBUTION

GOAL

Your organization must ensure privacy and security safeguards are in place for data sharing, electronic transmission, and distribution of data among members and organizations of your research team.

Explain your organizational safeguards. Examples are:

- Policies and procedures on how you secure PII shared among the research team
- Policies and procedures to ensure your organization follows CMS' cell suppression policy, such as in creating analytical extracts for research members
- Methods you use to track access and use of CMS data

Explain your personnel/staffing safeguards. Examples are:

- Policies and procedures you have that define data access privileges for specific staff members of a research team, such as a Principal Investigator, Data Custodian, other research analysts, administrative support, IT/computer support and volunteers (*Note: all volunteers assisting with a project must have a direct reporting relationship with a lead researcher*)

Explain your technical and physical safeguards. Examples are:

- Your approach to managing or limiting access to specific workstations, servers, data directories, or data files
- Your password management programs
- Your staff authentication protocols
- Your log-on/log-off protocols
- Your intrusion prevention protocols (measures to prevent access following specified number of failed access attempts)

- Your use of encryption standards, practices, polices if permitted on hard media devices or your organization's standards for the physical removal, transfer or disclosure of data

STEP 3: DATA REPORTING AND PUBLICATION

GOAL

Your organization must ensure that all analysis, findings, presentations, reports, and publications using CMS research data files adhere to specific requirements of the DUA (refer to section 9 in the DUA).

GUIDANCE

Explain how your organization ensures compliance with the publication requirements of the DUA. Note that for research involving Medicare Part D data, organizations must agree not to identify pharmacies, pharmacies, providers, prescribers or health plans.

STEP 4: COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

GOAL

Your organization must ensure that it has policies and procedures in place to destroy the data files upon completion of the research and that you have safeguards to ensure the data are protected when researchers terminate their participation in research projects.

Explain your organizational safeguards. Examples are:

- The methods you have put in place for ensuring changes to the research team are being managed, such as communicating project staffing changes to CMS
- Your policies and procedures for conducting staff exit meetings, including those with organizations you collaborate with for this particular project
- Your approach to notifying information technology support staff about blocking access to research staff or organization to all permitted data resources used for this project study and DUA

Explain your personnel/staffing safeguards. Examples are:

- Meetings you have with organizational and project-level privacy managers to ensure exiting staff are debriefed on privacy and security protection protocols
- The procedures you have in place to ensure the return of passkeys, swipe cards, and other media that permit access to data storage and research facilities

Explain your technical and physical safeguards. Examples are:

- The methods that you have put in place to ensure staff no longer have access to the data files upon completion of the research
- Policies and procedures that your organization has developed to complete the Certificate of Destruction form
- Policies and procedures that your organization has developed to ensure original data files or derivatives thereof will not be used following completion of the research project

APPENDIX: ADDITIONAL GUIDANCE FOR COMPLETING YOUR DATA MANAGEMENT PLAN

Scenarios

Various scenarios may apply to how research teams organize themselves to complete their research protocols. The examples provided below are meant to prompt your thinking about how your data environment is structured. Please note that these are just a few examples of scenarios and not meant to be an exhaustive list. Consider specific organizational, personnel, and technical safeguards for your organization's scenario when reviewing a data management plan.

BELOW WE HAVE PROVIDED EXAMPLES OF SCENARIOS THAT MAY APPLY TO YOUR ORANIZATION

Step 1: PHYSICAL POSSESSION AND STORAGE OF CMS DATA FILES

- In the proposed research, the data management plan will limit access to/distribution of CMS data files to a team within the same organization, or within a single administrative unit (department, office), which is under a single administrative supervisor
- The data management plan calls for distributing/sharing CMS data files 1) among multiple departments/locations within a single organization, or 2) across one or more distinct organizations

Step 2: DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

- Our data management plan proposes to store and maintain all original and backup CMS data files (and any derivatives made thereof for analytical use) on standalone, non-networked computer(s) in one or more physical locations
- The data management plan proposes to deploy original CMS data files on systems within our organization, with multiple simultaneous users, who may work in one or more physical locations
- Either or both of the above scenarios may apply, and the data management plan allows for staff to download and capture abstracts of the original CMS data files to their own computer

Step 3: DATA REPORTING AND PUBLICATION

- For the proposed research, the data management plan will clearly state how your organization will request approval from CMS prior to publishing study findings that include statistics, beneficiary, or facility level data to the public

Step 4: COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

- The subject research protocol and data management plan includes staff exit/termination policies and procedures that have been developed by my organization
- The subject research protocol and data management plan is governed by staff exit/termination policies and procedures that have been developed by my organization and supplemented by the research team
- Either 1 or 2 above applies, plus other external organizations are collaborating on this research protocol and their exit protocols are relevant to this step

REFERENCES

For more information, see the CMS matrix drawn from the *CMS Whitepaper Series, Volume 2, Paper 1, Security Standards Matrix*, pages 10–11. You can also reference the *Instructions for Completing the Data Use Agreement (DUA)* form for additional information.

The organizational and personnel/staffing safeguards are adapted from the "Administrative and Physical" safeguards within the Health Insurance *Portability and Accountability Act (HIPAA) Security Rule. The technic*al

Step 1—PHYSICAL POSSESSION AND STORAGE OF CMS DATA FILES

- NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology* System http//csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF
- NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
- NIST SP 800-2 *Engineering Principles for Information Technology Security (Baseline for Achieving Security)* http//csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf
- NIST SP 800-30 *Risk Management Guide for Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* http//csrc.nist.gov/publications/drafts/draft-SP800-53.pdf
- FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* http//csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- NIST SP 800-12 chapter 5 *An Introduction to Computer Security The NIST Handbook* http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Step 2—DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* http//csrc.nist.gov/publications/drafts/draft-SP800-53.pdf
- NIST SP 800-12 chapters 3, 15, 17 *An Introduction to Computer Security The NIST Handbook* http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
- NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF
- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* http//csrc.nist.gov/publications/drafts/draft-SP800-53.pdf
- NIST SP 800-63 *Recommendation for Electronic Authentication* http//csrc.nist.gov/publications/drafts/draft-sp800-63.pdf

Step 3—DATA REPORTING AND PUBLICATION

- NIST SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems* http//csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
- NIST SP 800-12 *An Introduction to Computer Security The NIST Handbook* http//csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Step 4—COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

- NIST SP 800-53 *Recommended Security Controls for Federal Information Systems* http//csrc.nist.gov/publications/drafts/draft-SP800-53.pdf
- NIST 800-88 *Guidelines for Media Sanitization* http//csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf